DETAILED ACTION

1. The response of 2/28/2008 was received and considered.

2. Claims 1-13 are pending.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with James Heintz (202-799-4000) on 5/22/2008.

The application has been amended as indicated below:

Please make the amendments to the specification as indicated in the following:

MARKED UP SPECIFICATION

Please amend paragraph 8 on page 8 as follows:

- randomly picking challenge parameters $r_i \in G$ and $a_{ij} \in Z_d$ for i = 1, … , k and j = 1, … , s+t (the number of input elements is now extended to s+t) and computing a challenge value $u_i = dr_i+a_{i1}g_1+\ldots[[a_{is}g_s+a_{is+1}y_1+\ldots+a_{is+t}y_t]]$ $\underline{a_{is}g_s+a_{is+1}x_1+\ldots+a_{is+t}x_t}$,

Please amend paragraphs 13 and 14 on page 8 as follows:

- verifying by the Signer whether $u_i = dr_i + a_{i1}g_1 + \ldots [[a_{is}g_s + a_{is+1}y_1 + \ldots + a_{is+t}y_t]]$ $a_{is}g_s + a_{is+1}x_1 + \ldots + a_{is+t}x_t$, and in the positive event, the Signer opens the commitment on the response value (V_i),

- verifying by the Verifier whether $vi = a_{i1}e_1 + \ldots [[a_{is}e_s + a_{is+1}y_1 + \ldots + a_{is+t}y_t]]$ $a_{is}e_s + a_{is+1}x_1 + \ldots + a_{is+t}x_t$.

Please REPLACE ALL CLAIMS with the amendments as indicated in the following:

MARKED UP CLAIMS (marked with respect to the claims submitted on 2/28/2008)

1. (Currently Amended) A method for generating an undeniable signature [[(y_1,..., y_t)]] on a set of data, the method comprising the following steps:

transforming the set of data to a sequence of a predetermined number of blocks [[(x_1, x_t)]], the blocks being members of an Abelian group, the transformation being a one way function; [[and]]

applying to each block a group homomorphism to obtain a resulting value, in which a number of elements of an initial group is larger than the number of elements of a destination group[[.]] ; and

storing the resulting value in a memory.

2. (Previously Presented) The method of claim 1, wherein the initial group is formed by a set of invertible integers modulo n, denoted as Z_n^*.

3. (Previously Presented) The method according to claim 2, wherein the group homomorphism computation is based on computation of a residue character (χ) on the set of invertible integers Z_n^*.

4. (Previously Presented) The method according to claim 3, wherein the residue character (χ) computation is based on a parameter (π) serving as a key.

5. (Previously Presented) The method according to the claim 4, wherein this key parameter (π) is determined by: $\pi \bullet \overline{\pi} = n$, $\overline{\pi}$ being the complex conjugate of π.

6. (Previously Presented) The method according to claim 2, wherein the group homomorphism computation is determined by raising an element of Z_n^* to the power of r(q-1), in which $n = p \bullet q$ such that $p = rd + 1$ and q are prime, gcd(r, d) = 1, gcd(q - 1, d) = 1, then by computing a discrete logarithm.

7. (Original) The method according to claim 6, wherein the group homomorphism is calculated using a factorization of n.

8. (Previously Presented) The method according to claim 1, wherein the length of the signature is dependent of the number of elements of the destination group and the number of blocks.

9. (Previously Presented) The method according to claim 4, wherein the parameter is a secret key on an asymmetric public/secret key pair.

10. (Currently Amended) A method of confirming by a Verifier an undeniable signature (y_1, ..., y_t) of a set of data (m) generated by a Signer taking into account a predefined security parameter of the confirmation protocol, this Signer having a public/secret key pair, this method comprising the following steps:

obtaining a personal value (ρ) from the Signer, this personal value being part of the public key (G, H, d, ρ, (e_1, ... e_s)) of the Signer;

extracting a first sequence of elements (e_1, ... e_s) from the public key;

generating a second sequence of elements (g_1, ... g_s) from the personal value (ρ);

generating a third sequence of elements (x_1, ..., x_t) from the set of data (m);

randomly picking challenge parameters $r_i \varepsilon G$ and $a_{ij} \varepsilon Z_d$ for i = 1, ... , k and j = 1, ..., s + t and computing a challenge value $u_i = dr_i + a_{i1}g_1 + ... [[a_{is}g_s+a_{is+1}y_1+\ldots+a_{is+t}y_t]]$ $a_{is}g_s+a_{is+1}x_1+\ldots+a_{is+t}x_t$;

sending by the Verifier the challenge value u_j to the Signer;

receiving from the Signer a commitment value (<v_i>), this commitment value (<v_i>) being calculated by the Signer based on a response value $v_i = f(u_i)$;

sending by the Verifier the challenge parameters r_i and a_{ij} to the Signer;

verifying by the Signer whether $u_i = dr_i + a_{i1}g_1 + ... [[a_{is}g_s+a_{is+1}y_1+\ldots+a_{is+t}y_t]]$ $a_{is}g_s+a_{is+1}x_1+\ldots+a_{is+t}x_t$, and in [[the]] a positive event, opening by the Signer the commitment on the response value (v_i)[[,]] ; and

verifying by the Verifier whether $v_i = a_{i1}e_1 + ... a_{is}e_s + [[a_{is+1}y_1 + ... + a_{is+t}y_t]]$ $a_{is+1}x_1+\ldots+a_{is+t}x_t$.

11. (Previously Presented) A method for denying to a Verifier by a Signer on an alleged non-signature (z1, ..., zt) of a set of data (m), this signature being supposedly generated according to claim 1 by the Signer, this Signer having a public/secret key pair, this method taking into account a predefined security parameter (ℓ) of the denial protocol and comprising the following steps:

obtaining by the Verifier a personal value (ρ) of the Signer, this personal value being part of the public key (G, H, d, ρ, (e_1, ... e_s)) of the Signer;

extracting by the Verifier a first sequence of elements (e_1, ... e_s) from the public key;

generating by the Verifier and the Signer a second sequence of elements (g_1, ... g_s) from the personal value (ρ);

generating by the Verifier and the Signer a third sequence of elements (x_1, ..., x_i) from the set of data (m);

calculating by the Signer a true signature (y_1,..., y_t); and

repeating the following steps ℓ times, ℓ being the predetermined security parameter;

randomly picking by the Verifier challenge parameters $r_j \varepsilon G$ and $a_{ji} \varepsilon Z_d$ for i = 1, ... , s and j = 1, ..., t and $\lambda \varepsilon Z_p^*$ where p is the smallest prime dividing d;

computing $u_j := dr_j + a_{j1}g_1 + ... a_{js}g_s + \lambda x_j$, and $w_j := a_{j1}e_1 + ... a_{js}e_s + \lambda z_j$ for j =1...t;

sending by the Verifier the challenge values u_j and w_j to the Signer;

computing by the Signer a response test value $TV_j := (z_j - y_j)\bullet$;

for each j = 1 to t, determining whether the test value $TV_j = 0$;

in [[the]] a negative event, calculating a test parameter λ_j according to the following formula: $w_j - v_j, = \lambda_j (z_j - y_j)$;

determining an intermediate value (IV), the intermediate value (IV) being equal to one valid test parameter (λ) and in case of no valid test parameter is found, selecting as the intermediate value (IV) a random value;

sending a commitment value CT based on the intermediate value (IV), to the Verifier;

sending by the Verifier the challenge parameters r_j , a_{ji} and test parameter (λ) to the Signer;

verifying by the Signer whether $u_j = dr_j + a_{j1}g_1 + ... a_{js}g_s + \lambda x_j$ and $w_j := a_{j1}e_1 + ... a_{js}e_s + \lambda z_j$ for j = 1 ... t hold, in [[the]] a positive event, the Signer opens the commitment on the intermediate value (IV) to the Verifier; and

verifying by the Verifier that the test parameter (λ) is equal to the intermediate value (IV).

12. (Previously Amended) The method of claim 11, in which the determination of the valid test parameter comprises a check whether (w_j-v_j,) and (z_j-y_j) are not equal to 0.

13. (Previously Amended) The method of claim 11, in which j > 1, the determination of the valid test parameter comprises a check whether (w_j-v_j) and (z_j-y_j) are not equal to 0, and that all of the test parameters are the same.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance:

a. Regarding claim 1, "Homomorphic Signatures Schemes" by **Johnson et al.** discloses that the RSA scheme is homomorphic (§1 & §5). Further, it is known that the RSA scheme operates on the abelian multiplicative group Z/mZ* (see **Google Answers** reference, p. 2, second to the last posting). U.S. Patent 6,292,879 to **Gennaro et al.** discloses Undeniable Certificates, which is an undeniable signature scheme. "RSA-Based Undeniable Signatures" by **Gennaro et al.** discloses undeniable signatures, including operating on a message using a one-way function and then applying the RSA encryption scheme (see p. 138, §3). Handbook of Applied Cryptography by **Menezes et al.** teaches the ElGamal signature scheme in the multiplicative group Z*p (an abelian group), applying a hash function (see p. 457, last ¶). *However, the prior art of record fails to teach or disclose, either alone or in combination, a group homomorphism to obtain a resulting value, in which a number of elements of an initial group is larger than the number of elements of a destination group, in combination with the other elements of the claim as a whole and as described on at least pp. 7-8 of the specification.*

b. Regarding claim 10, U.S. Patent 5,373,558 to **Chaum et al**. discloses confirming by a verifier a signature (Fig. 4), including obtaining a personal value from the signing (public key, see message 21 in Fig. 2), but lacks extracting a first sequence of elements from the public key, generating a second sequence of elements, randomly picking challenge parameters, computing a challenge value and verifying by the Signer, as claimed. "Convertible Undeniable Signature Scheme" by **Yun et al**. discloses an

undeniable signature confirmation protocol, §3.2, but lacks the above steps. U.S. Patent 6,292,897 to **Gennaro et al**. also discloses an undeniable signature verification method (col. 4, lines 31-48), but also lacks the above steps, as claimed. "RSA-Based Undeniable Signatures" by **Gennaro et al.** discloses undeniable signatures, specifically the confirmation protocol, where elements from a public key are extracted (Sw), random values are picked (i,j), a challenge value is computed (Q) (see p. 139, Fig. 1), a commitment is created (commit(A) and the verifier verifies that A corresponds to the value committed to by P (p. 140, ¶1), but lacks the remainder of the steps discussed above, as claimed. Handbook of Applied Cryptography by **Menezes et al.** teaches the general structure of zero-knowledge protocols, where a first party chooses a commitment (which can consist of multiple parts or iterations), a second party randomly selects a challenge, the first party sends a response and the second party checks the response to verify that the first party knows a secret without requiring the first party to reveal the secret (see p. 409, #3 and Note 10.25 (iv)). *However, the prior art of record fails to teach or disclose, either alone or in combination, the specific equations claimed as they relate to the values such as the public key, specifically, the claimed generating by the a second sequence of elements from the personal value, randomly picking the challenge parameters in sets G and Zd as claimed, and the computing of the values Ui and Vi by the signer and verifier, respectively, in combination with the other elements of the claim as a whole and as described on p. 8 of the specification.*

c. Regarding claim 11, Menezes is the closes prior art, but *differs from the claimed invention for at least the same reasons given above for claim 10.* Further, *the claim*

differs from the prior art of ***Chaum***, ***Yun*** *and* ***Gennaro*** *by claiming at least the steps of extracting by the Verifier a first sequence of elements from the public key, generating by the Verifier and Signer a second sequence of elements from the personal value, randomly picking by the Verifier challenge parameters from G and Zd (with respect to the public key), as specifically claimed, in combination with the other elements of the claim as a whole and as described in at least p. 9-10 of the specification.*

d. Claims 2-9 are allowable based on their dependence upon claim 1 and claims 12-13 are allowable based on their dependence upon claim 11.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

May 22, 2008
/Michael J Simitoski/
Primary Examiner, Art Unit 2134